明 細 書

通信システム及びそれを用いた通信方法

技術分野

[0001] 本発明は、通信システム及びそれを用いた通信方法に係り、特に暗号鍵を光ファイバ通信により共有する量子暗号鍵の配布を行う通信システム及びそれを用いた通信方法に関する。

背景技術

[0002] 近年、インターネットの爆発的普及、電子商取引の実用化を迎え、通信の秘密保持・改ざん防止や個人の認証などのために、暗号技術の社会的な必要性が高まっている。現在、DES(Data Encryption Standard)暗号のような共通鍵方式やRSA(Rivest Shamir Adleman)暗号をはじめとする公開鍵方式が広く用いられている。しかし、これらの方式は「計算量的安全性」にその基盤を置いている。つまり、現行の暗号方式は計算機ハードウェアと暗号解読アルゴリズムの進歩に常に脅かされている。特に、銀行間のトランザクションや軍事・外交にかかわる情報などの極めて高い安全性が要求される分野では、原理的に安全な暗号方式が実用になればそのインパクトは大きい。

[0003] 情報理論で無条件安全性が証明されている暗号方式に、ワンタイムパッド法がある。ワンタイムパッド法は通信文と同じ長さの暗号鍵を用い、暗号鍵を1回で使い捨てることが特徴である。下記非特許文献1で、ワンタイムパッド法に使用する暗号鍵を安全に配送する具体的なプロトコルが提案された。これを契機に量子暗号の研究が盛んになっている。量子暗号は物理法則が暗号の安全性を保証するため、計算機の能力の限界に依存しない究極の安全性保証が可能になる。現在検討されている量子暗号は1ビットの情報を単一光子の状態として伝送するものである。このため、伝送路である光ファイバにより光子の状態が変化すると量子暗号の安全性は大きく損なわれる。

[0004] 従来の量子暗号装置(下記特許文献2参照)では、第2のステーション(送信)側で光パルスを光路差のある干渉計を用いて時間的に2分割し、互いの位相差を変調す

ることにより暗号鍵となる乱数ビットを表現し、第1のステーション(受信)側で2分割された光パルスを再び干渉させることにより伝送された乱数ビットを再生している。このため、第2のステーション(送信)側と第1のステーション(受信)側で用いる干渉計の光路差は完全に等しくなければならない。また、伝送路で偏光状態が変動すると干渉の明瞭度が低下し、受信誤り率の増大につながる。量子暗号では受信誤り率の増大を盗聴者検出の手段としているため、伝送路での偏光状態の変化に起因する受信誤り率の増大は盗聴者の発見確率を減少させ、結果として量子暗号の安全性を低下させる。また、量子暗号装置では、盗聴行為が存在したものと仮定して、第1のステーション及び第2のステーションの間で共有した乱数ビット群から、盗聴された危険性のあるビット量に相当する情報量を破棄し、共有乱数データの秘匿性を確実なものにする。この際、破棄するべき情報量は受信誤り率によって一様に定まる。受信誤り率が高い場合には、より多くの情報量を破棄する必要があり、最終的な共有乱数データ量が減少、つまり量子暗号の暗号鍵生成速度が劣化することになる。

[0005] 上述のような問題を解決するため、下記特許文献1またはこれを簡略にした下記特許文献3および下記非特許文献2に記載されているように、ファラデーミラーを用いて偏光方向の変動を補償する量子暗号装置が発明されている。この装置では、まず受信者が時間的に分割され偏光が直交した光パルスを送信者に送り、送信者はファラデーミラーを用いて送られてきた光の進行方向を反転させ、同時に偏光方向を90度回転させた後、分割された光パルスの間に位相変調器により位相差を与えて受信者に送り返すという構成をとっている。このような折り返し構成により、光パルスを時間的に分割する干渉計と時間的に再び結合させる干渉計は同一のものになるため、干渉計の光路差が光パルスの往復時間より長い時間だけ一定に保たれれば明瞭度の高い干渉が得られる。よく知られているように、ファラデーミラーで反射された光は、途中の伝送路でいかなる偏光状態の攪乱を受けても戻った光の偏光方向は初めの状態に直交するため、伝送路での偏光状態の攪乱に対しても干渉計の明瞭度は損なわれることはなく、量子暗号の安全性は保障される。

特許文献1:特表2000—517499号

特許文献2:特許第2951408号

特許文献3:USP 6, 188, 768B1

非特許文献1:ベネット(Bennett)、ブラッサード(Brassard)著 IEEEコンピュータ、システム、信号処理国際会議〔IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore, India, p. 175(1984)〕

非特許文献2:リボルディ(Ribordy)、ガウチャー(Gautier)、ジサン(Gisin)、グィナルド(Guinnard)、ツビンデン(Zbinden)著 エレクトロニクスレターズ(Electronics Letters) 34巻 2116−2117頁(1998)

発明の開示

[0006] しかしながら、上記特許文献2に開示された量子暗号装置にはいくつかの問題がある。

[0007] 第一の問題点は送信者の用いる位相変調器を実現することが困難だということである。これは以下に起因する。

[0008] 送信者は位相変調器で時間的に分割された光パルスの間に位相差を与えるが、この位相変調器は以下の条件を満たす必要がある。

(1)量子暗号で唯一安全性が数学的に証明されているプロトコルである、上記非特許文献1で開示されたBB84プロトコルでは位相差として0度、90度、180度、270度の4種類を与えることが必要である。

(2)分割された時間間隔内で位相変調を与える。光パルスが伝送中に干渉性を保つためにはパルスの時間間隔を数ナノ秒以下にする必要があり、位相変調器の変調帯域は少なくとも1GHz程度は必要となる。

(3)伝送路を通った光の偏光状態は変動しているので、あらゆる偏光に対して同じ変調特性を示すことが必要である。

[0009] 現在実用化されている位相変調器で上述の条件を全て満たすのは困難である。例えば、1GHz以上の変調帯域を持つ位相変調器としてはニオブ酸リチウムを用いたものとInPなどの化合物半導体を用いたものがあり、損失が小さいことからニオブ酸リチウムが広く使われている。しかし、これらの位相変調器は、一般に偏光依存性を持ち、特定の偏光を指定して用いるのが通常である。また、偏光無依存型の位相変調器も存在するが、これは0度と180度の位相変調に必要な電圧が偏光方向に依らな

くなるように設計されるため、中間の90度や270度での特性は保証されない。

[0010] 第二の問題点はファラデーミラーが磁気光学素子であるため、将来期待される光回路の集積化に不向きなことである。これは、磁気光学素子が通常の集積光回路の材料であるシリコン・ガラス・ニオブ酸リチウムなどでは構成できないためである。上記特許文献3に開示された方法によれば偏光依存性を持つ位相変調器も使用できるが、ファラデーミラーを必要とする。

[0011] 第三の問題点はファラデーミラーの回転角精度及び温度に依存して暗号鍵生成速度が変化するということである。これは、以下に起因する。

[0012] 上記特許文献2で開示された量子暗号装置では、光パルスを時間的に分割する干渉計と時間的に再び結合させる干渉計を同一のものにするため、送信者が光パルスの偏光方向を厳密に90度回転させる必要がある。この偏光回転角が90度よりずれると、第1のステーション(受信機)において復路で往路と同一の経路を通る光パルスが増加し、干渉の明瞭度が劣化するとともに暗号鍵生成速度が劣化する。

[0013] ここで、一般に市販されているファラデーミラーの偏光回転角の精度誤差は±3度程度、最も特性の良いものでも±1度程度である。偏光回転角が90度から3度ずれると約3%の光子が結合せずに干渉計を通過し、その分暗号鍵生成の精度が劣化する。

[0014] また、ファラデー効果による偏光回転角は温度依存性を持ち、ファラデー素子の温度が変化すると偏光回転角も同様に変化する。この温度依存性の一般値は−0.12度／℃である。つまり素子の温度が25℃変化するとファラデーミラーによる偏光回転角は3度変化し、同様に暗号鍵生成速度の劣化を引き起こす。

[0015] 本発明の目的は、伝送路での偏光状態の攪乱に対して安全性が損なわれない折り返し構成をとりながら、暗号鍵生成速度の劣化を引き起こすファラデーミラーを用いずに第2のステーション(送信機)における90度の偏光回転を精度良く実現し、また偏光依存性のある位相変調器が使用できる通信システム及びそれを用いた通信方法を提供することにある。

[0016] 上記目的を達成するために、本発明の通信システム及びそれを用いた通信方法は、

〔1〕通信システムにおいて、時間的に分割された光パルスを伝送路に放出し、伝送路から折り返してきた光パルス間の位相差を測定する手段を備えた第1のステーションと、光の媒体となる前記伝送路と、光パルスの進行方向を反転させる手段と分割された光パルス間に送信する乱数ビット値に対応した位相差を与える手段と入射した光パルスを直交偏光成分に分割し、直交偏光成分間に180度の位相差を与える手段と各々の偏光を90度回転させる手段を有し、さらに直交偏光成分を合成し前記伝送路に再び光パルスを放出する手段を有する第2のステーションからなることを特徴とする。

[0017] 〔2〕上記〔1〕記載の通信システムにおいて、前記位相差を与える手段として位相変調器を用い、この位相変調器への信号電圧を変化させることにより、直交偏光成分間に180度の位相差を与えることを特徴とする。

[0018] 〔3〕上記〔1〕記載の通信システムにおいて、前記送信する乱数ビット値に対応した位相差を与える手段と直交偏光成分間に180度の位相差を与える手段に同一の位相変調器を用い、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする。

[0019] 〔4〕上記〔1〕記載の通信システムにおいて、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射し、位相差を与えた後偏光を各々90度回転させ、再び合成することを特徴とする。

[0020] 〔5〕上記〔4〕記載の通信システムにおいて、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分が位相変調器に入射するまでの距離を各々の偏光成分で異なる値とし、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする。

[0021] 〔6〕上記〔4〕記載の通信システムにおいて、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射するまでの光路が、定偏波光ファイバで構成されていることを特徴とする。

[0022] 〔7〕上記〔6〕記載の通信システムにおいて、前記定偏波光ファイバの偏光軸を入射した光パルスの直交偏光成分の電界ベクトルの向きに合わせることにより、前記分割

された偏光成分が合成される際にもとの偏光方向から90度回転されていることを特徴とする。

[0023] 〔8〕上記〔4〕、〔5〕又は〔6〕記載の通信システムにおいて、前記直交偏光成分間に180度の位相差を与える手段と偏光を各々90度回転させる手段としてファラデー回転子を用いることを特徴とする。

[0024] 〔9〕上記〔1〕記載の通信システムにおいて、前記光パルスを直交成分に分割する手段及び合成する手段として偏光ビームスプリッタを使用し、前記偏光ビームスプリッタの偏光回転の90度からのずれ成分が出力される端子が無反射終端されていることを特徴とする。

[0025] 〔10〕上記〔1〕から〔9〕の何れか1項記載の通信システムにおいて、前記第2のステーションが、直交偏光成分を合成し伝送路に再び光パルスを放出する際、光パルスの強度が1ビットあたり1光子以下になるように減衰させる手段を有し、量子暗号鍵を配布することを特徴とする。

[0026] 〔11〕通信方法において、第1のステーションにより、時間的に分割された光パルスを伝送路に放出し、伝送路から折り返してきた光パルス間の位相差を測定し、第2のステーションにより、光の媒体となる前記伝送路と、光パルスの進行方向を反転させる手段と分割された光パルス間に送信する乱数ビット値に対応した位相差を与える手段と入射した光パルスを直交偏光成分に分割し、直交偏光成分間に180度の位相差を与える手段と各々の偏光を90度回転させる手段を有し、さらに直交偏光成分を合成し、前記伝送路に再び光パルスを放出することを特徴とする。

[0027] 〔12〕上記〔11〕記載の通信方法において、前記位相差を与える手段として位相変調器を用い、この位相変調器への信号電圧を変化させることにより、直交偏光成分間に180度の位相差を与えることを特徴とする。

[0028] 〔13〕上記〔11〕記載の通信方法において、前記送信する乱数ビット値に対応した位相差を与える手段と直交偏光成分間に180度の位相差を与える手段に同一の位相変調器を用い、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする。

[0029] 〔14〕上記〔11〕記載の通信方法において、前記入射した光パルスを直交偏光成分

に分割した後、前記分割された偏光成分を位相変調器の両端から入射し、位相差を与えた後偏光を各々90度回転させ、再び合成することを特徴とする。

[0030] 〔15〕上記〔14〕記載の通信方法において、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分が位相変調器に入射するまでの距離を各々の偏光成分で異なる値とし、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする。

[0031] 〔16〕上記〔14〕記載の通信方法において、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射するまでの光路が、定偏波光ファイバで構成されていることを特徴とする。

[0032] 〔17〕上記〔16〕記載の通信方法において、前記定偏波光ファイバの偏光軸を入射した光パルスの直交偏光成分の電界ベクトルの向きに合わせることにより、前記分割された偏光成分が合成される際にもとの偏光方向から90度回転されていることを特徴とする。

[0033] 〔18〕上記〔14〕、〔15〕又は〔16〕記載の通信方法において、前記直交偏光成分間に180度の位相差を与える手段と偏光を各々90度回転させる手段としてファラデー回転子を用いることを特徴とする。

[0034] 〔19〕上記〔11〕記載の通信方法において、前記光パルスを直交成分に分割する手段及び合成する手段として偏光ビームスプリッタを使用し、前記偏光ビームスプリッタの偏光回転の90度からのずれ成分が出力される端子が無反射終端されていることを特徴とする。

[0035] 〔20〕上記〔11〕から〔19〕の何れか1項記載の通信方法において、前記第2のステーションが、直交偏光成分を合成し伝送路に再び光パルスを放出する際、光パルスの強度が1ビットあたり1光子以下になるように減衰させる手段を有し、量子暗号鍵を配布することを特徴とする。

[0036] 特に、本発明の通信システム及びそれを用いた通信方法は、時間的に分割された光パルスを伝送路に放出し、伝送路から折り返してきた光パルス間の位相差を測定する手段を備えた第1のステーション(受信機)と、光の媒体となる前記伝送路と、光

パルスの進行方向を反転させる手段と分割された光パルス間に送信する乱数ビット値に対応した位相差を与える手段と入射した光パルスを直交偏光成分に分割し、直交偏光成分間に180度の位相差を与える手段と各々の偏光を90度回転させる手段を有し、さらに直交偏光成分を合成する際に前記90度回転からのずれ成分を除去する手段を有し、前記伝送路に再び光パルスを放出する際、パルスの強度が1ビットあたり1光子以下になるように減衰させる手段を有する第2のステーション(送信機)からなる。

図面の簡単な説明

[0037] [図1]本発明の量子暗号システムの実施の形態を示す概略構成図である。

[図2]本発明の量子暗号システムの第1のステーションの実施の形態を示す構成図である。

[図3]本発明の量子暗号システムの第2のステーションの実施の形態を示す構成図である。

[図4]本発明の量子暗号システムの第2のステーション内を伝播する光パルスの時間順序の説明図である。

[図5]本発明の量子暗号システムの第2のステーションの実施の第2の形態を示す構成図である。

[図6]本発明の量子暗号システムの偏光ビームスプリッタにおける偏光成分の分離と合成を説明する図である。

発明を実施するための最良の形態

[0038] 本発明の第1の効果としては、上記第2のステーション(送信機)内で、直交する2つの偏光成分に分けた上で、片方の偏光成分を90度回転させていることにより、位相変調器に入射する光の偏光方向は同一でかつ一定とすることができ、偏光依存性のある位相変調器を用いることができる量子暗号システムを提供することができる。

[0039] 本発明の第2の効果としては、光の偏光方向を元の光とは直交させ、さらに異なる直交偏光成分の位相を反転させることにより、ファラデーミラーを用いることなく、伝送路での偏光状態を攪乱に対して安全性が損なわれない量子暗号システムを提供することができる。

[0040] 本発明の第3の効果としては、ファラデーミラーを用いることなく上記第2のステーション(送信機)入射時と送出時の光信号の偏光方向を直交させることにより、環境温度の変化やファラデー素子の精度によって暗号鍵生成速度が変化しない量子暗号システムを提供することができる。

[0041] 本発明の第4の効果としては、上記第2のステーション(送信機)内で、直交する2つの偏光成分に分け、各々の偏光成分を90度回転させて合成する際に前記90度回転からのずれ成分を除去することによって、上記第2のステーション内での偏光回転角精度によって暗号鍵生成速度が変化しない量子暗号システムを提供することができる。

[0042] 入射した光パルスを直交偏光成分に分割し、直交偏光成分間に180度の位相差を与え、各々の偏光を90度回転させ、分割した直交偏光成分を合成する際に前記90度回転からのずれを除去することにより伝送路での偏光状態の攪乱に対して安全性が損なわれない折り返し構成をとりながら、暗号鍵生成速度の劣化の要因となるファラデーミラーを用いることなく上記90度の偏光回転を精度良く実現し、また偏光依存性のある位相変調器が使用できる量子暗号システムを提供する。

実施例

[0043] 本発明の実施の形態について図面を参照して詳細に説明する。

[0044] 図1は本発明の実施例としての通信システム(量子暗号システム)の概略構成図である。

[0045] この図に示すように、本発明の量子暗号システムは、第1のステーション(受信機)1、伝送路2、第2のステーション(送信機)3からなり、第1のステーション1から光パルスを伝送路2に放出し、第2のステーション3で変調した後、伝送路2に戻し、第1のステーション1でビット値を測定する。

[0046] このように、第1のステーション1は時間的に分割された光パルスを伝送路2に放出し、伝送路2から折り返してきた光パルス間の位相差を測定する手段を有する。

[0047] そこで、第1のステーション1から伝送路2へ放出された時間的に2分割された光パルスは、伝送路2で偏光状態に攪乱を受けた後、第2のステーション3に入射する。第2のステーション3内で、光パルスは、直交する2つの偏光成分に分けられ、一つの

偏光成分はそのまま第一の位相変調器に入る。もう一方の偏光成分は偏光方向を90度回転された後、第二の位相変調器に入射する。第一の位相変調器は第1のステーション1で時間的に分割された光パルス間に乱数ビットの値に対応して位相差を与え、第二の位相変調器は光パルス間に第一の位相変調器が与えたのと同じ大きさの位相差を与える。同時に異なる同一の光パルスの直交偏光成分の間には180度の位相差を与えるようにする。第一の位相変調器の出力は偏光方向を90度回転された後、第二の位相変調器の出力と合成される。合波された光は減衰器で1ビットあたりの光子数が1以下になるまで減衰された後、再び伝送路2を戻される。以上の過程を経て第1のステーション1に戻った時間的に2分割された光パルス間には乱数ビットに対応した位相差が与えられ、偏光方向が反転している。第1のステーション1内の干渉計により光パルス間の位相差を測定することにより、送信された乱数ビットの値を知ることができる。

[0048] 伝送路2での攪乱にかかわらず、第1のステーション1から放出した偏光に対して直交した偏光が第1のステーション1に戻ることは以下のように数式を用いて説明できる。偏光を2次元のベクトル

[0049] [数1]

$$\vec{E}=\begin{pmatrix} E_x \\ E_y \end{pmatrix}$$

で表すと、偏光の攪乱は偏光の回転

[0050] [数2]

$$R_0(\theta)=\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

と直交偏光成分間の位相差

[0051] [数3]

$$R_i(\phi)=\begin{pmatrix} \exp[i\phi/2] & 0 \\ 0 & \exp[-i\phi/2] \end{pmatrix}$$

で引き起こされる。伝送路2を通過した後の偏光の状態は一般に

[0052] [数4]

$$\vec{E}' = \begin{pmatrix} E_x' \\ E_y' \end{pmatrix} = R_i(\gamma) R_0(\beta) R_i(\alpha) \vec{E}$$

と表せることが知られている。

ここで、光の進行方向を反転すると偏光は$E_x' \rightarrow E_x'$、$E_x' \rightarrow -E_y'$のように変化する。さらに、直交偏光成分の間に180度の位相差を与え、偏光方向を90度回転させると伝送路2に再び放出される偏光状態は

[0053] [数5]

$$\vec{E}'' = \begin{pmatrix} E_y' \\ E_x' \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \vec{E}'$$

と表せる。再び伝送路2を通過させると伝送後に得られる偏光は次のようになる。

[0054] [数6]

$$\vec{E}^{(1)} = R_i(\alpha) R_0(\beta) R_i(\gamma) \vec{E}'' = R_i(\alpha) R_0(\beta) R_i(\gamma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} R_i(\gamma) R_0(\beta) R_i(\alpha) \vec{E}$$

ここで、

[0055] [数7]

$$\begin{pmatrix} \exp[i\phi/2] & 0 \\ 0 & \exp[-i\phi/2] \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \exp[i\phi/2] & 0 \\ 0 & \exp[-i\phi/2] \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

を使うと、

[0056] [数8]

$$\vec{E}^{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \vec{E} = \begin{pmatrix} E_y \\ E_x \end{pmatrix}$$

となり、伝送路2での偏光の攪乱によらず元の偏光に直交した偏光が戻ることがわかる。このようなことが成立する条件は光パルスが伝送路2を往復する時間内で伝送路特性の性質が変化しないことである。例えば、光ファイバ50kmを光パルスが往復するのに必要な時間は0．5msであるが、光ファイバの偏光状態は数秒から数時間変化しないことが知られており、この条件は満足される。

[0057] 図2は本発明の実施例としての受信機(第1のステーション)の構成図である。

[0058] この図に示すように、第1のステーション1は光源11、サーキュレータ12、ビームスプリッタ13、偏波コントローラ14、位相変調器15、偏光ビームスプリッタ16および光子検出器17，18からなる。

[0059] 光源11を出た光パルスはサーキュレータ12を通りビームスプリッタ13で2分割される。2分割された光の一方は位相変調器15を通って偏光ビームスプリッタ16に入射する。分割されたもう一方の光も偏光ビームスプリッタ16の別の端子に入るが、偏光の向きは偏波コントローラ14により90度回転されている。分割された光は偏光ビームスプリッタ16により合波された後、時間的に2分割された光パルスとして伝送路2に放出される。ビームスプリッタ13で分割されてから偏光ビームスプリッタ16により合波されるまでの光路差は時間的に2分割された光パルスの時間差が光のパルス幅より長く、パルス間隔より短い時間になるように設定される。

[0060] 伝送路2を通過した光は第2のステーション3に入る。

[0061] 図3は本発明の実施例としての送信機(第2のステーション)の構成図であり、図4は本発明の実施例としての第2のステーション内を伝搬する光パルスの時間順序の説明図である。

[0062] この図に示すように、第2のステーション3は偏光ビームスプリッタ31、定偏波光ファイバ32，33、位相変調器34、光減衰器35から構成される。

[0063] 入射した光は、第2のステーション3内で光減衰器35を通った後、偏光ビームスプリッタ31で直交した偏光成分に分離され、図4に示すように、4つの光パルス301ー304になる。図中、光パルス301は第1の分割された光パルスの一偏光成分、光パルス302は第1の分割された光パルスの直交偏光成分、光パルス303は第2の分割された光パルスの一偏光成分、光パルス304は第2の分割された光パルスの直交偏光成分にそれぞれ対応する。各々の偏光成分は偏光ビームスプリッタ31の端子312，313に現れるが、端子312，313はそれぞれ電界ベクトルの向きを遅軸に合わせた定偏波光ファイバ32，33に結合される。定偏波光ファイバ32，33は位相変調器34の両端にそれぞれ接続される。電界ベクトルの向きを定偏波光ファイバ32，33の遅軸に合わせているため、位相変調器34に入射する偏光の向きは全ての光パルスで同一

になる。このとき、一方の偏光成分に対応したパルス301と303は他の偏光成分に対応した光パルス302と304より時間Tだけ早く位相変調器34に入射するように定偏波光ファイバ32，33の長さを設定する。ただし、時間Tは光パルスの時間幅より大きく、2分割された光パルスの時間間隔より小さくする。位相変調器34を出た光パルス301と303は定偏波光ファイバ33を通って偏光ビームスプリッタ31の端子313に入る。また、位相変調器34を出た光パルス302と304は定偏波光ファイバ32を通って偏光ビームスプリッタ31の端子312に入る。光パルス301と302、303と304は同じ定偏波光ファイバ32，33を逆方向に進行したので偏光ビームスプリッタ31には同じ時刻に入射し、合波される。合波された光パルスは光減衰器35を通り、2分割された光パルスを合わせた平均光子数が0．1から1の間に設定された値になるように減衰された後、伝送路2を逆に伝播して第1のステーション1に戻る。

[0064] 上記の第2のステーション3において偏光を90度回転させるために定偏波光ファイバ32，33の遅軸に電界ベクトルを合わせたが、ファイバ内で偏光が保存される方向であればどの方向に合わせても良い。また、無偏波の単一モード光ファイバあるいは空間を伝播させ、波長板などからなる偏光調整器を用いて偏光を回転させても良い。

[0065] 光減衰器35は第2のステーション3側に置いたが第2のステーション3から第1のステーション1へ向かう平均光子数が0．1から1の間に設定された値になるように第1のステーション1側に置くようにしても良い。

[0066] そこで、図4に示されるように、端子312と313を出た光は、位相変調器34までの光路長が異なるため、図4(A)から(F)まで時間が経過する間の異なった時刻に位相変調器34に入射する。このため、パルス間隔に同期して位相変調器34に印加する電圧を変化させることによって各々の光パルスに異なった位相差を与えることができる。各光パルスに与える位相差を表1に示すように設定する。

[0067] [表1]

ビット値	位相(301)	位相(302)	位相(303)	位相(304)
0	0°	180°	0°	180°
	0°	180°	90°	270°
1	0°	180°	180°	0°
	0°	180°	270°	90°

時間的に分割された光パルス301と303の間に、乱数ビットの値が"0"のとき0度または90度の位相差を与え、"1"のとき180度または270度の位相差を与える。光パルス301と303の直交偏光成分である光パルス302と304の間には光パルス301と303の間と同じ大きさの位相差を与え、同時に光パルス301と302、303と304の間には180度の位相差を与える。

[0068] 各々の光パルスは偏光ビームスプリッタ31から出たときは異なる端子に戻るため、偏光ビームスプリッタ31からは元とは直交した偏光で端子311から出射する。

[0069] 各々の光パルスを分離、合成する際に偏光ビームスプリッタを使用することによって偏光の90度回転の精度によらず安定した暗号鍵生成が行えることは以下のように説明できる。

[0070] 偏光ビームスプリッタにおける偏光成分の分離と合成に関して図6を用いて説明する。偏光ビームスプリッタとは、広義では入射光を2つの直交する偏光成分に分離する光学系の総称であるが、ここでは光通信分野で一般的に用いられている構成を取り上げる。この構成は、図6(A)に示すように、2つのプリズムと誘電体多層膜を組み合わせることにより、反射・屈折の際のブリュースター角を利用して、入射面と直交するs偏光成分614だけを反射して入射面内にあるp偏光成分615だけを透過する。伝送路より偏光ビームスプリッタ61の端子611に入射した光パルスは、各々の偏光成分(s偏光成分616, p偏光成分617)が端子612と613に分離されて出射される。

[0071] 各々の偏光成分は90度偏光回転されて偏光ビームスプリッタ61から出た時と異なる端子に戻るが、この際回転角が90度よりずれており、純粋な直線偏光状態ではないと仮定する。具体的には、図6(B)に示すように端子622より光が出射した場合、出力時には純粋なs偏光626のみの直線偏光となっており、90度偏光回転されて端子623に入射する際には純粋なp偏光627のみの直線偏光となっているはずであるが

、偏光回転角のずれのため、一部s偏光成分628も含んだ偏光状態となっている。しかし、この光のうちp偏光成分627は偏光ビームスプリッタ62を透過して(p偏光成分625)端子621より伝送路へと送り返されるが、s偏光成分628は偏光ビームスプリッタ62において反射され(s偏光成分629)端子624に送り出される。

[0072] 一方、偏光ビームスプリッタの端子633からp偏光637が出射される場合を図6(C)に示す。この場合も同様に端子632にs偏光638のみ入射するはずが、一部p偏光成分636も含んでいる。この光のうちs偏光成分638は偏光ビームスプリッタ63で反射され(s偏光成分635)端子631より伝送路へと送り返されるが、p偏光成分636は偏光ビームスプリッタ63を透過して(p偏光成分639)端子634から出射される。ここで端子624、634を終端しておけばこれらの光が干渉計に戻ることはない。第2のステーション内部での偏光回転角が90度よりずれると、第1のステーションで適切な変調を施すことができないため、干渉計の明瞭度が損なわれ暗号鍵生成精度が劣化するが、以上のように第2のステーション内部において偏光成分の分離・合成に偏光ビームスプリッタを使用すると、この劣化を防ぐことができる。

[0073] 以上の例では4端子の偏光ビームスプリッタに関して述べたが、3端子の偏光ビームスプリッタで端子624, 634に対応する部分に無反射終端処理が施されていても同様の効果が得られる。また偏光ビームスプリッタの構成も上記構成に限らず、一軸性光学結晶を使用したものやファイバ融着型のものでもよい。

[0074] 以上のようにして第2のステーション3では光の進行方向の反転、偏光の90度回転、偏光の直交成分間に180度の位相差の3つの操作を行っている。特に、本実施の形態では直交する偏光成分の光が同一の経路を逆方向に伝播するため、光路における攪乱は打ち消されて安定な第2のステーション3が実現できる。

[0075] 伝送路2を逆方向に伝播した光パルスは伝送路2を経て再び第1のステーション1に入る。光パルスは偏光ビームスプリッタ16で偏光方向により光路が分けられる。第1のステーション1に戻った時間的に2分割された光パルスの偏光は第1のステーション1を出たときのものと直交しているから、第1のステーション1での光路差は打ち消されてビームスプリッタ13には同時に入射する。片方の光路で偏波コントローラ14により偏光が90度回転しているからビームスプリッタ13上で2つの光路を通った光の間で

干渉が起きる。受信者は位相変調器15で0度または90度の位相変調を選択して印加する。第2のステーション3でビット値“0”に対応して光パルス301と303との間に0度の位相変調を行ったとすると、受信者が位相変調器15で0度の位相変調を行ったときには光子検出器17でのみ光子が観測される。第2のステーション3でビット値“1”に対応して光パルス301と303との間に180度の位相変調を行ったとすると、受信者が位相変調器15で0度の位相変調を行ったときには光子検出器18でのみ光子が観測される。

[0076] 同様に、第2のステーション3でビット値“0”に対応して光パルス301と303との間に90度の位相変調を行ったとすると、受信者が位相変調器15で90度の位相変調を行ったときには光子検出器17でのみ光子が観測され、第2のステーション3でビット値“1”に対応して光パルス301と303との間に270度の位相変調を行ったとすると、受信者が位相変調器15で90度の位相変調を行ったときには光子検出器18でのみ光子が観測される。このように第2のステーション3の位相変調に対して第1のステーション1で行う位相変調の大きさが適切であるとき、光子検出器17と18のいずれで光子が検出されるかにより、第1のステーション1において送信されたビット値を確定することができる。具体的には、第1のステーション1で行う位相変調の深さは、0度、90度、180度、270度のいずれかである。

[0077] 上記の実施の形態において、直交偏光成分間に180度の位相差を与える手段と偏光を各々90度回転させる手段としてファラデー回転子を用いて構成することができる。そのための構成を第2の実施の形態として図5に示す。

[0078] 本発明の第2の実施の形態では、ファラデー回転子51が必要になるが、位相変調器34は時間的に分割された光パルスのうち光パルス303と304に等しい大きさの位相を与えればよいので、位相変調器34に印加する電圧の周期を2倍にでき、電圧制御回路の構成が容易になるという効果を奏する。

[0079] なお、本発明は上記実施例に限定されるものではなく、本発明の趣旨に基づき種々の変形が可能であり、これらを本発明の範囲から排除するものではない。

産業上の利用可能性

[0080] 本発明は、暗号鍵を光ファイバ通信により共有する量子暗号システムとして利用可

能である。

請求の範囲

[1] 時間的に分割された光パルスを伝送路に放出し、伝送路から折り返してきた光パルス間の位相差を測定する手段を備えた第1のステーションと、光の媒体となる前記伝送路と、光パルスの進行方向を反転させる手段と分割された光パルス間に送信する乱数ビット値に対応した位相差を与える手段と入射した光パルスを直交偏光成分に分割し、直交偏光成分間に180度の位相差を与える手段と各々の偏光を90度回転させる手段を有し、さらに直交偏光成分を合成し前記伝送路に再び光パルスを放出する手段を有する第2のステーションからなることを特徴とする通信システム。

[2] 請求項1記載の通信システムにおいて、前記位相差を与える手段として位相変調器を用い、該位相変調器への信号電圧を変化させることにより、直交偏光成分間に180度の位相差を与えることを特徴とする通信システム。

[3] 請求項1記載の通信システムにおいて、前記送信する乱数ビット値に対応した位相差を与える手段と直交偏光成分間に180度の位相差を与える手段に同一の位相変調器を用い、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする通信システム。

[4] 請求項1記載の通信システムにおいて、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射し、位相差を与えた後偏光を各々90度回転させ、再び合成することを特徴とする通信システム。

[5] 請求項4記載の通信システムにおいて、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分が位相変調器に入射するまでの距離を各々の偏光成分で異なる値とし、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする通信システム。

[6] 請求項4記載の通信システムにおいて、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射するまでの光路が、定偏波光ファイバで構成されていることを特徴とする通信システム。

[7] 請求項6記載の通信システムにおいて、前記定偏波光ファイバの偏光軸を入射し

た光パルスの直交偏光成分の電界ベクトルの向きに合わせることにより、前記分割された偏光成分が合成される際にもとの偏光方向から90度回転されていることを特徴とする通信システム。

[8] 請求項4、5又は6記載の通信システムにおいて、前記直交偏光成分間に180度の位相差を与える手段と偏光を各々90度回転させる手段としてファラデー回転子を用いることを特徴とする通信システム。

[9] 請求項1記載の通信システムにおいて、前記光パルスを直交成分に分割する手段及び合成する手段として偏光ビームスプリッタを使用し、前記偏光ビームスプリッタの偏光回転の90度からのずれ成分が出力される端子が無反射終端されていることを特徴とする通信システム。

[10] 請求項1から9の何れか1項記載の通信システムにおいて、前記第2のステーションが、直交偏光成分を合成し伝送路に再び光パルスを放出する際、光パルスの強度が1ビットあたり1光子以下になるように減衰させる手段を有し、量子暗号鍵を配布することを特徴とする通信システム。

[11] 第1のステーションにより、時間的に分割された光パルスを伝送路に放出し、伝送路から折り返してきた光パルス間の位相差を測定し、

第2のステーションにより、光の媒体となる前記伝送路と、光パルスの進行方向を反転させる手段と分割された光パルス間に送信する乱数ビット値に対応した位相差を与える手段と入射した光パルスを直交偏光成分に分割し、直交偏光成分間に180度の位相差を与える手段と各々の偏光を90度回転させる手段を有し、さらに直交偏光成分を合成し、前記伝送路に再び光パルスを放出することを特徴とする通信方法。

[12] 請求項11記載の通信方法において、前記位相差を与える手段として位相変調器を用い、該位相変調器への信号電圧を変化させることにより、直交偏光成分間に180度の位相差を与えることを特徴とする通信方法。

[13] 請求項11記載の通信方法において、前記送信する乱数ビット値に対応した位相差を与える手段と直交偏光成分間に180度の位相差を与える手段に同一の位相変調器を用い、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする通信方法。

[14] 請求項11記載の通信方法において、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射し、位相差を与えた後偏光を各々90度回転させ、再び合成することを特徴とする通信方法。

[15] 請求項14記載の通信方法において、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分が位相変調器に入射するまでの距離を各々の偏光成分で異なる値とし、信号電圧を時間的に変化させることによって乱数ビット値に対応した位相差と直交偏光成分間の180度の位相差を同時に与えることを特徴とする通信方法。

[16] 請求項14記載の通信方法において、前記入射した光パルスを直交偏光成分に分割した後、前記分割された偏光成分を位相変調器の両端から入射するまでの光路が、定偏波光ファイバで構成されていることを特徴とする通信方法。

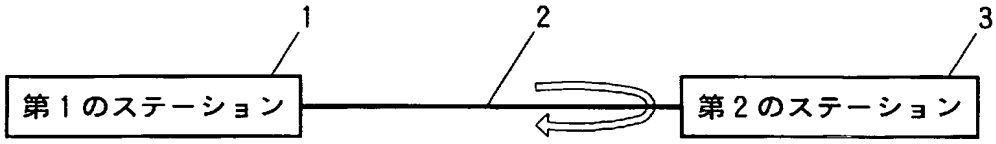
[17] 請求項16記載の通信方法において、前記定偏波光ファイバの偏光軸を入射した光パルスの直交偏光成分の電界ベクトルの向きに合わせることにより、前記分割された偏光成分が合成される際にもとの偏光方向から90度回転されていることを特徴とする通信方法。

[18] 請求項14、15又は16記載の通信方法において、前記直交偏光成分間に180度の位相差を与える手段と偏光を各々90度回転させる手段としてファラデー回転子を用いることを特徴とする通信方法。

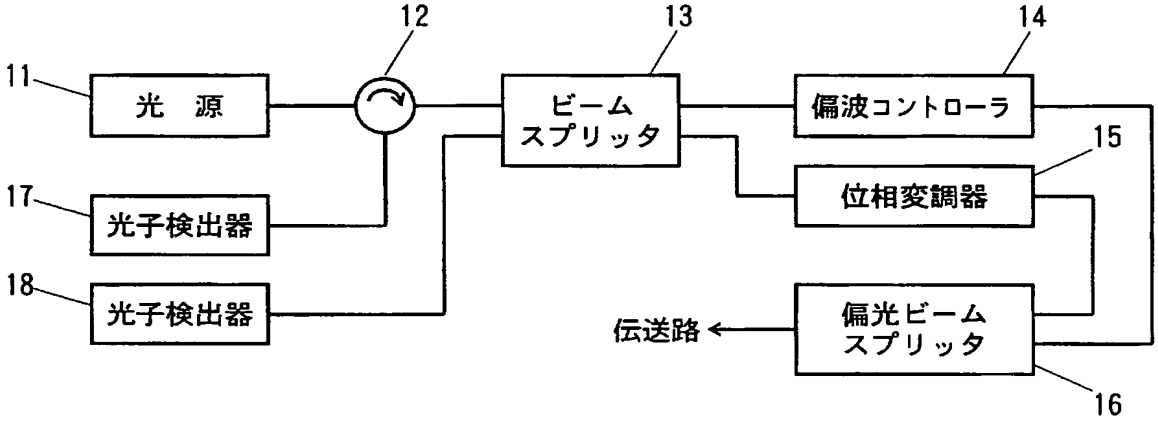
[19] 請求項11記載の通信方法において、前記光パルスを直交成分に分割する手段及び合成する手段として偏光ビームスプリッタを使用し、前記偏光ビームスプリッタの偏光回転の90度からのずれ成分が出力される端子が無反射終端されていることを特徴とする通信方法。

[20] 請求項11から19の何れか1項記載の通信方法において、前記第2のステーションが、直交偏光成分を合成し伝送路に再び光パルスを放出する際、光パルスの強度が1ビットあたり1光子以下になるように減衰させる手段を有し、量子暗号鍵を配布することを特徴とする通信方法。

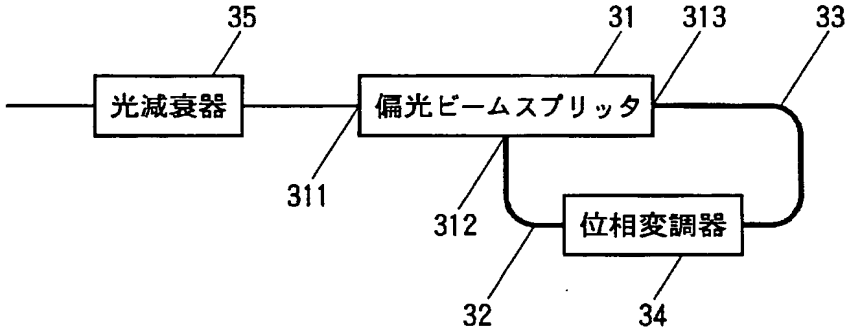
[図1]


1
2
3
第１のステーション
第２のステーション

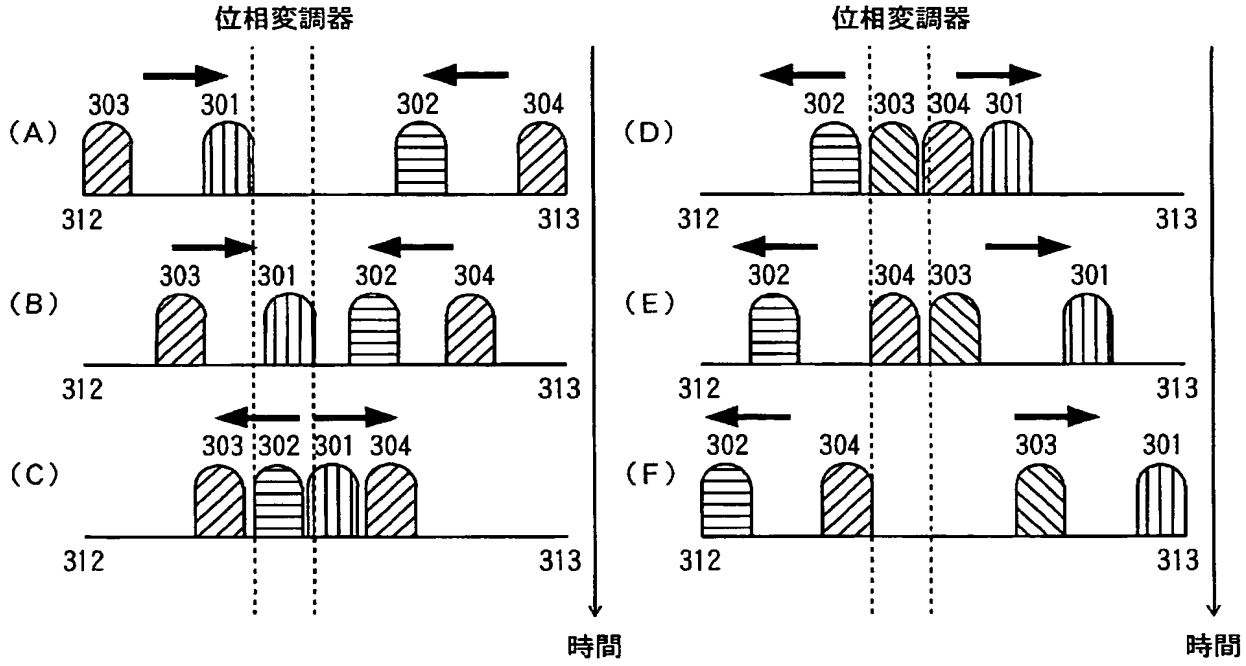
[図2]


12
13
14
11
光　源
ビーム
スプリッタ
偏波コントローラ
15
17
光子検出器
位相変調器
18
光子検出器
伝送路
偏光ビーム
スプリッタ
16

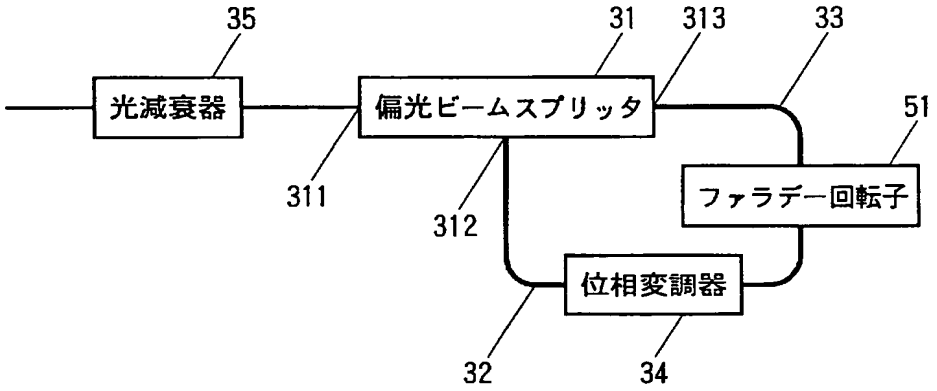
[図3]


35
31
313
33
光減衰器
偏光ビームスプリッタ
311
312
位相変調器
32
34

[図4]

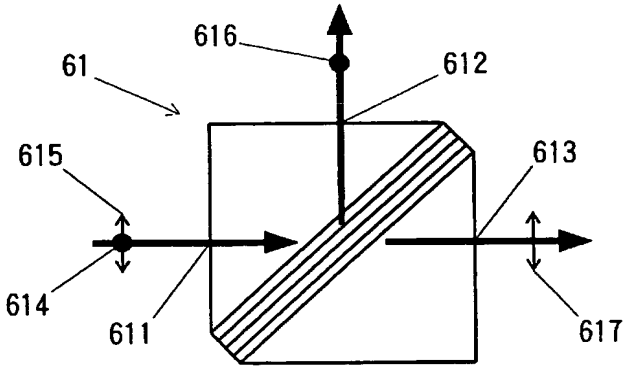

位相変調器
(A)
303
301
302
304
312
313
(B)
303
301
302
304
312
313
(C)
303
302
301
304
312
313
時間
位相変調器
(D)
302
303
304
301
312
313
(E)
302
304
303
301
312
313
(F)
302
304
303
301
312
313
時間

[図5]

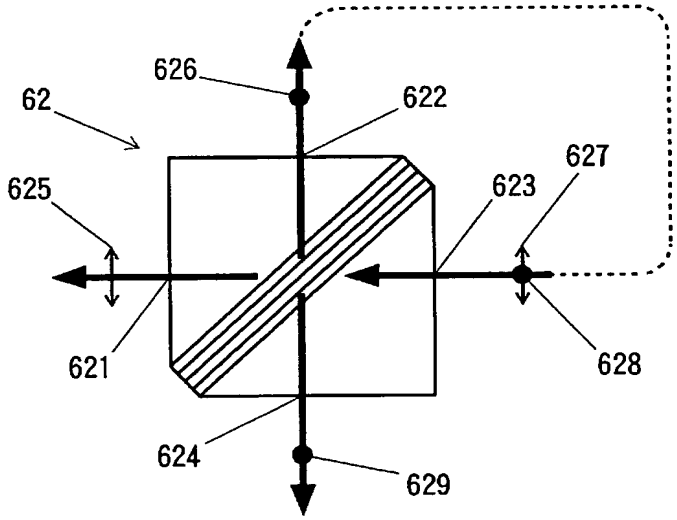

35
光減衰器
31
313
33
偏光ビームスプリッタ
51
ファラデー回転子
311
312
位相変調器
32
34

[図6]

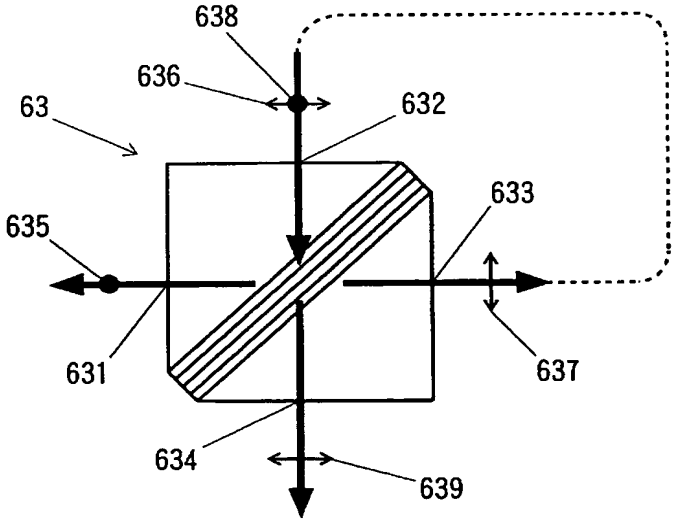
(A)


616
61
612
615
613
614
611
617

(B)


626
62
622
627
625
623
621
628
624
629

(C)


638
636
63
632
633
635
631
637
634
639

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/017681

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Jitsuyo Shinan Toroku Koho 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Takeshi NISHIOKA et al., "Kanryugata Ryoshiken Haifu", 2002 Nen Ango to Joho Security Symposium Yokoshu, Volume I of II, 29 January, 2002 (29.01.02), pages 43 to 48	1-5,10-15, 20 6-9,16-19
Y	JP 2003-289298 A (Nihon University), 10 October, 2003 (10.10.03), Par. Nos. [0030] to [0036]; Fig. 1 (Family: none)	6-8,16-18
Y	JP 2002-340566 A (Fujikura Ltd.), 27 November, 2002 (27.11.02), Claim 7; Par. Nos. [0025] to [0038]; Fig. 4 (Family: none)	9,19

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 February, 2005 (07.02.05)	22 February, 2005 (22.02.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告	国際出願番号　PCT／JP2004／017681

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／12

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国登録実用新案公報	1994－2005年
日本国実用新案登録公報	1996－2005年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	西岡毅他，還流型量子鍵配布，2002年暗号と情報セキュリティシンポジウム予稿集，Volume I of II，2002.01.29，p.43-48	1-5, 10-15, 20
Y		6-9, 16-19
Y	JP 2003-289298 A（学校法人日本大学）2003.10.10, 段落【0030】-【0036】，図1（ファミリーなし）	6-8, 16-18
Y	JP 2002-340566 A（株式会社フジクラ）2002.11.27, 【請求項7】，段落【0025】-【0038】，図4（ファミリーなし）	9, 19

☐ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
07．02．2005	22.2.2005

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	中里　裕正	5M　3365
	電話番号　03－3581－1101　内線　3597	